

CLAIMS

What is claimed is:

- 1           1.       An apparatus comprising:  
2           an initialization storage to initialize a chipset in a secure environment for an  
3           isolated execution mode, the secure environment having a plurality of executive entities  
4           and being associated with an isolated memory area accessible by at least one processor,  
5           the at least one processor having a plurality of threads and operating in one of a normal  
6           execution mode and the isolated execution mode, the executive entities including a  
7           processor executive (PE) handler; and  
8           a PE handler storage to store PE handler data corresponding to the PE handler,  
9           the PE handler data including a PE handler image to be loaded into the isolated memory  
10          area after the chipset is initialized, the loaded PE handler image corresponding to the  
11          PE handler.
- 1           2.       The apparatus of claim 1 further comprises:  
2           a thread count storage to store a thread count indicating number of threads  
3           currently initialized for operation in the isolated execution mode;  
4           a thread count updater coupled to the thread count storage to update the thread  
5           count;  
6           a mode storage to store a chipset mode indicating a mode of operation of the  
7           chipset; and  
8           a mode write circuit coupled to the mode storage to write the chipset mode to  
9           the mode storage.
- 1           3.       The apparatus of claim 2 further comprising:  
2           an identifier log storage to store cryptographic identifiers of the executive  
3           entities loaded into the isolated execution mode, the cryptographic identifiers being  
4           read only when in lock;  
5           a log lock storage to store a lock pattern indicating the identifiers in lock; and  
6           a lock circuit coupled to the identifier log storage and the log lock storage to  
7           lock the identifiers based on the lock pattern.

1           4.       The apparatus of claim 3 further comprising:  
2           a platform key storage to store a platform key used in handling the executive  
3 entities; and  
4           a scratch storage to store isolated settings used to configure the isolated  
5 execution mode.

1           5.       The apparatus of claim 4 wherein the executive entities further include a  
2 processor executive (PE) and an operating system executive (OSE).

1           6.       The apparatus of claim 5 wherein the chipset mode is one of an  
2 initialization waiting mode to indicate the chipset is waiting for initialization, a PE  
3 initialization in-progress mode to indicate the PE is being executed, a PE initialization  
4 completion mode to indicate the PE is completed, an OSE loaded mode to indicate the  
5 OSE has been loaded, a closing mode to indicate the isolated execution mode is closed,  
6 and a failure mode to indicate a failure.

1           7.       The apparatus of claim 6 wherein the initialization storage returns an  
2 updated thread count when the chipset mode does not represent the failure mode and to  
3 return a current thread count when the chipset mode represents the failure mode, the  
4 updated thread count being one of an incremented thread count and a decremented  
5 thread count.

1           8.       The apparatus of claim 7 wherein the initialization storage comprises:  
2 an enrollment storage to return the incremented thread count when one of the  
3 threads enrolls in the isolated execution mode; and  
4 a withdrawal storage to return the decremented thread count when one of the  
5 enrolled threads withdraws from the isolated execution mode.

1           9.       The apparatus of claim 8 wherein the mode write circuit writes the  
2 chipset mode corresponding to a failure mode into the mode storage when the thread  
3 count reaches a thread limit.

1           10.     The apparatus of claim 1 wherein the PE handler data further include a  
2 cryptographic PE handler identifier, a PE handler size, and a PE handler address.

1           11.     The apparatus of claim 6 wherein the PE handler storage is a read-only  
2 memory.

1           12.     The apparatus of claim 6 wherein the platform key is returned when the  
2 platform key storage is read in the initialization waiting mode.

1           13.     The apparatus of claim 12 wherein the platform key is programmed to a  
2 random value.

1           14.     The apparatus of claim 13 further comprising:  
2 a status storage to store a status value of an isolated unlock pin used in setting  
3 platform settings.

1           15.     The apparatus of claim 4 wherein the isolated settings include an  
2 isolated base value, an isolated length value, and a processor executive entry address,  
3 the isolated base and length values defining the isolated memory area.

1           16.     A method comprising:  
2 initializing a chipset in a secure environment for an isolated execution mode by  
3 an initialization storage, the secure environment having a plurality of executive entities  
4 and being associated with an isolated memory area accessible by at least one processor,  
5 the at least one processor having a plurality of threads and operating in one of a normal  
6 execution mode and the isolated execution mode, the executive entities including a  
7 processor executive (PE) handler; and  
8 storing PE handler data corresponding to the PE handler in a PE handler storage,  
9 the PE handler data including a PE handler image to be loaded into the isolated memory  
10 area after the chipset is initialized, the loaded PE handler image corresponding to the  
11 PE handler.

1           17.     The method of claim 16 further comprises:  
2           storing a thread count in a thread count storage indicating number of threads  
3     currently initialized for operation in the isolated execution mode;  
4           updating the thread count when the initialization storage is accessed;  
5           storing a chipset mode indicating a mode of operation of the chipset in a mode  
6     storage; and  
7           writing the chipset mode into the mode storage.

1           18.     The method of claim 17 further comprising:  
2           storing cryptographic identifiers of the executive entities loaded into the isolated  
3     execution mode, the identifiers being read only when in lock;  
4           storing a lock pattern indicating the identifiers in lock; and  
5           locking the identifiers based on the lock pattern.

1           19.     The method of claim 18 further comprising:  
2           storing a platform key used in handling the executive entities in a platform key  
3     storage; and  
4           storing isolated settings used to configure the isolated execution mode.

1           20.     The method of claim 19 wherein the executive entities further include a  
2     processor executive (PE) and an operating system executive (OSE).

1           21.     The method of claim 20 wherein the chipset mode is one of an  
2     initialization waiting mode to indicate the chipset is waiting for initialization, a PE  
3     initialization in-progress mode to indicate the PE is being executed, a PE initialization  
4     completion mode to indicate the PE is completed, an OSE loaded mode to indicate the  
5     OSE has been loaded, a closing mode to indicate the isolated execution mode is closed,  
6     and a failure mode to indicate a failure.

1           22.     The method of claim 21 wherein initializing the chipset comprises

2           returning an updated thread count when the chipset mode does not represent the  
3 failure mode, the updated thread count being one of an incremented thread count and a  
4 decremented thread count; and

5           returning a current thread count when the chipset mode represents the failure  
6 mode.

1           23.     The method of claim 22 wherein initializing the chipset further  
2 comprises:

3           returning the incremented thread count when one of the threads enrolls in the  
4 isolated execution mode; and

5           returning the decremented thread count when one of the enrolled threads  
6 withdraws from the isolated execution mode.

1           24.     The method of claim 23 wherein writing the chipset mode comprises  
2 writing the chipset mode corresponding to a failure mode when the thread count reaches  
3 a thread limit.

1           25.     The method of claim 16 wherein the PE handler data further include a  
2 PE handler identifier, a PE handler size, and a PE handler address.

1           26.     The method of claim 21 wherein the PE handler storage is read-only  
2 memory.

1           27.     The method of claim 21 wherein the platform key is returned when the  
2 platform key storage is read in the initialization waiting mode.

1           28.     The method of claim 27 wherein the platform key is programmed to a  
2 random value.

1           29.     The method of claim 28 further comprising:  
2           storing a status value of an isolated unlock pin used to unlock and allow  
3 platform setting.

1           30.     The method of claim 19 wherein the isolated settings include an isolated  
2     base value, an isolated length value, and a processor executive entry address, the  
3     isolated base and length values defining the isolated memory area.

1           31.     A computer program product comprising:  
2             a machine useable medium having computer program code embedded therein,  
3     the computer program product having:  
4             computer readable program code for initializing a chipset in a secure  
5     environment for an isolated execution mode by an initialization storage, the secure  
6     environment having a plurality of executive entities and being associated with an  
7     isolated memory area accessible by at least one processor, the at least one processor  
8     having a plurality of threads and operating in one of a normal execution mode and the  
9     isolated execution mode, the executive entities including a processor executive (PE)  
10    handler; and  
11            computer readable program code for storing PE handler data corresponding to  
12    the PE handler in a PE handler storage, the PE handler data including a PE handler  
13    image to be loaded into the isolated memory area after the chipset is initialized, the  
14    loaded PE handler image corresponding to the PE handler.

1           32.     The computer program product of claim 31 further comprises:  
2             computer readable program code for storing a thread count in a thread count  
3     storage indicating number of threads currently initialized for operation in the isolated  
4     execution mode;  
5             computer readable program code for updating the thread count when the  
6     initialization storage is accessed;  
7             computer readable program code for storing a chipset mode indicating a mode  
8     of operation of the chipset in a mode storage; and  
9             computer readable program code for writing the chipset mode into the mode  
10    storage.

1           33.     The computer program product of claim 32 further comprising:

2 computer readable program code for storing cryptographic identifiers of the  
3 executive entities loaded into the isolated execution mode, the identifiers being read  
4 only when in lock;  
5 computer readable program code for storing a lock pattern indicating the  
6 identifiers in lock; and  
7 computer readable program code for locking the identifiers based on the lock  
8 pattern.

1 34. The computer program product of claim 33 further comprising:  
2 computer readable program code for storing a platform key used in handling the  
3 executive entities in a platform key storage; and  
4 computer readable program code for storing isolated settings used to configure  
5 the isolated execution mode.

1 35. The computer program product of claim 34 wherein the executive  
2 entities further include a processor executive (PE) and an operating system executive  
3 (OSE).

1 36. The computer program product of claim 35 wherein the chipset mode is  
2 one of an initialization waiting mode to indicate the chipset is waiting for initialization,  
3 a PE initialization in-progress mode to indicate the PE is being executed, a PE  
4 initialization completion mode to indicate the PE is completed, an OSE loaded mode to  
5 indicate the OSE has been loaded, a closing mode to indicate the isolated execution  
6 mode is closed, and a failure mode to indicate a failure.

1 37. The computer program product of claim 36 wherein the computer  
2 readable program code for initializing the chipset comprises  
3 computer readable program code for returning an updated thread count when the  
4 chipset mode does not represent the failure mode, the updated thread count being one of  
5 an incremented thread count and a decremented thread count; and  
6 computer readable program code for returning a current thread count when the  
7 chipset mode represents the failure mode.

1           38.     The computer program product of claim 37 wherein the computer  
2 readable program code for initializing the chipset further comprises:  
3           computer readable program code for returning the incremented thread count  
4 when one of the threads enrolls in the isolated execution mode; and  
5           computer readable program code for returning the decremented thread count  
6 when one of the enrolled threads withdraws from the isolated execution mode.

1           39.     The computer program product of claim 38 wherein the computer  
2 readable program code for writing the chipset mode comprises computer readable  
3 program code for writing the chipset mode corresponding to a failure mode when the  
4 thread count reaches a thread limit.

1           40.     The computer program product of claim 31 wherein the PE handler data  
2 further include a PE handler cryptographic identifier, a PE handler size, and a PE  
3 handler address.

1           41.     The computer program product of claim 36 wherein the PE handler  
2 storage is a read-only memory.

1           42.     The computer program product of claim 36 wherein the platform key is  
2 returned when the platform key storage is read in the initialization waiting mode.

1           43.     The computer program product of claim 42 wherein the platform key is  
2 programmed to a random value.

1           44.     The computer program product of claim 43 further comprising:  
2           computer readable program code for storing a status value of an isolated unlock  
3 pin used to unlock and allow platform settings.



1           45.     The computer program product of claim 34 wherein the isolated settings  
2 include an isolated base value, an isolated length value, and a processor executive entry  
3 address, the isolated base and length values defining the isolated memory area.

1           46.     A system comprising:  
2           at least one processor having a plurality of threads and operating in one of a  
3 normal execution mode and an isolated execution mode;  
4           a memory having an isolated memory area accessible to the at least one  
5 processor in the isolated execution mode; and  
6           a chipset circuit coupled to the at least one processor and the memory  
7 comprising:  
8           an initialization storage to initialize a chipset in a secure environment for the  
9 isolated execution mode, the secure environment having a plurality of executive entities  
10 and being associated with the isolated memory area, the executive entities including a  
11 processor executive (PE) handler, and  
12           a PE handler storage to store PE handler data corresponding to the PE handler,  
13 the PE handler data including a PE handler image to be loaded into the isolated memory  
14 area after the chipset is initialized, the loaded PE handler image corresponding to the  
15 PE handler.

1           47.     The system of claim 46 wherein the chipset circuit further comprises:  
2           a thread count storage to store a thread count indicating number of threads  
3 currently operating in the isolated execution mode,  
4           a thread count updater coupled to the thread count storage to update the thread  
5 count when the initialization storage is accessed;  
6           a mode storage to store a chipset mode indicating a mode of operation of the  
7 chipset; and  
8           a mode write circuit coupled to the mode storage to write the chipset mode into  
9 the mode storage.

1           48.     The system of claim 47 wherein the chipset circuit further comprises:

2 an identifier log storage to store cryptographic identifiers of the executive  
3 entities operating in the isolated execution mode, the identifiers being read only when  
4 in lock;  
5 a log lock storage to store a lock pattern indicating the identifiers in lock; and  
6 a lock circuit coupled to the identifier log storage and the log lock storage to  
7 lock the identifiers based on the lock pattern.

1 49. The system of claim 48 wherein the chipset circuit further comprises:  
2 a platform key storage to store a platform key used in handling the executive  
3 entities; and  
4 a scratch storage to store isolated settings used to configure the isolated  
5 execution mode.

1 50. The system of claim 49 wherein the executive entities further include a  
2 processor executive (PE) and an operating system executive (OSE).

1 51. The system of claim 50 wherein the chipset mode is one of an  
2 initialization waiting mode to indicate the chipset is waiting for initialization, a PE  
3 initialization in-progress mode to indicate the PE is being executed, a PE initialization  
4 completion mode to indicate the PE is completed, an OSE loaded mode to indicate the  
5 OSE has been loaded, a closing mode to indicate the isolated execution mode is closed,  
6 and a failure mode to indicate a failure.

1 52. The system of claim 51 wherein the initialization storage returns an  
2 updated thread count when the chipset mode does not represent the failure mode and to  
3 return a current thread count when the chipset mode represents the failure mode, the  
4 updated thread count being one of an incremented thread count and a decremented  
5 thread count.

1 53. The system of claim 52 wherein the initialization storage comprises:  
2 an enrollment storage to return the incremented thread count when one of the  
3 threads enrolls in the isolated execution mode; and

4 a withdrawal storage to return the decremented thread count when one of the  
5 enrolled threads withdraws from the isolated execution mode.

1 54. The system of claim 53 wherein the mode write circuit writes the chipset  
2 mode corresponding to a failure mode into the mode storage when the thread count  
3 reaches a thread limit.

1 55. The system of claim 46 wherein the PE handler data further include a PE  
2 handler cryptographic identifier, a PE handler size, and a PE handler address.

1 56. The system of claim 51 wherein the PE handler storage is a non-volatile  
2 memory.

1 57. The system of claim 51 wherein the platform key is returned when the  
2 platform key storage is read in the initialization waiting mode.

1 58. The system of claim 57 wherein the platform key is programmed to a  
2 random value.

1 59. The system of claim 58 wherein the chipset circuit further comprises:  
2 a status storage to store a status value of an isolated unlock pin used to unlock  
3 and allow platform settings.

1 60. The system of claim 49 wherein the isolated settings include an isolated  
2 base value, an isolated length value, and a processor executive entry address, the  
3 isolated base and length values defining the isolated memory area.